

CIVIL SERVICE OF JAMAICA
JOB DESCRIPTION AND SPECIFICATION
COURT ADMINISTRATION DIVISION

JOB TITLE:	Data Protection Officer
JOB GRADE:	GMG/SEG 3/Band 9
DEPARTMENT/DIVISION:	Court Administration Division
BRANCH	Executive Office,
REPORTS TO:	Director of Court Administration
ACCOUNTABLE TO:	Director of Court Administration
MANAGES:	N/A

This document is validated as an accurate and true description of the job as signified below:

Employee

Date

Manager/Supervisor

Date

Head of Department/Division

Date

1. STRATEGIC OBJECTIVES OF THE DIVISION

TBD

2. JOB PURPOSE

Under the leadership and direction of the Director of Court Administration, the Data Protection Officer will support the development of Data Protection/Privacy policies, procedures, controls and guidance which ensures the Judiciary compliance with the Data Protection Act 2020, Data Protection Standards and any applicable globally standards.

3. KEY OUTPUTS

- Data Protection and privacy legal frameworks, policies, procedures and systems researched, developed and implemented
- Data Protection/Privacy Governance Frameworks and strategies coordinated
- Data Protection and privacy advice provided
- Robust and comprehensive Data Protection controls coordinated
- Data Protection and privacy training coordinated and provided
- Reports, Submissions/Notes, technical papers, and publications prepared and issued
- Stakeholder Relationships and Alliances maintained
- Annual/Quarterly/Monthly performance Reports prepared
- Individual work plans developed

4. KEY RESPONSIBILITY AREAS

Technical/Professional Responsibilities

- Provides research capabilities to develop and implement Data Protection and privacy policies, procedures and systems in support of the Judiciary's core function.
- Coordinates and owns any changes to policies and working practices relevant to the Data Protection and privacy function.
- Identifies and addresses areas where the Judiciary needs to review strategy, policy or procedure, or increase colleague awareness and training in Data Protection and Privacy.
- Researches, designs and implements Data Protection/Privacy Governance Frameworks and strategies to manage the use of Judiciary's data in compliance with the legislative framework, standards and guidelines
- Provides advice on all matters relating to the general Data Protection and privacy impact assessments issues by ensuring the Judiciary compliance with applicable legal framework and policy guidelines.
- Designs, implements and monitors robust and comprehensive Data Quality and Protection controls across the Judiciary that supports the Judiciary's ICT landscape.

- Devises, updates and reports on data and information management controls, issues, breaches and major incidents pertaining to the Judiciary's core function.
- Maintains appropriate records to enable the Judiciary to liaise effectively and legally with the relevant supervisory authorities where applicable.
- Develops and manages data protection compliance frameworks by ensuring compliance checking activities are undertaken and compliance checking schedules are in place.
- Develops and implements protocols and frameworks for coordinating and conducting data privacy audits.
- Conducts regular reviews of the Judiciary's data processing operations and the accessibility of clients' personal data.
- Coordinates systems that ensure appropriate assignment of responsibilities in relation to the management of data and information and the processing and protection of personal data.
- Receives, processes and escalates requests from the public relating to who has accessed personal data and for what purpose the data was used.
- Applies a systematic approach to decision making and problem solving by calculating and identifying risks involved in various aspects of the functional area.
- Works with key internal stakeholders in the review of work processes/projects and related data concerning the Judiciary's core function to ensure compliance with local data protection and privacy laws where applicable.
- Monitors the development and changes to Jamaican data protection and privacy laws; and makes recommendations to the Data Privacy and Information Governance to bolster processes and systems concerning information/data systems in the Judiciary.
- Develops and delivers Data Protection and privacy training to various stakeholders in the Judiciary.
- Monitors the industry landscape to keep visibility on evolutions, trends, and best practices related to Data Privacy.
- Develops and implements strategies and initiatives to ensure engagement with key internal and external stakeholders relating Data Protection and privacy matters.
- Collaborates with internal and external Information Security functionaries to raise stakeholder awareness of data privacy and security issues concerning the Judiciary.
- Collaborates with internal and external Information Security functionaries in the development and implementation of procedures and systems to maintain records of all data assets and management of data security incidents.
- Promotes and embeds good Data quality and Information security principles across the Judiciary and related stakeholder groupings/partners.
- Keeps abreast of Data Protection and Privacy initiatives to ensure adherence to international standards and competitiveness.

Management/Administrative Responsibilities

- Develops Individual Work Plans based on alignment to the overall plan for the section.
- Participates in meetings, seminars, workshops and conferences as required.

- Prepares reports and programme documents as required.
- Maintains customer service principles, standards and measurements.

Human Resources Responsibilities

- Contributes to and maintains a system that fosters a culture of teamwork, employee empowerment and commitment to the Division's and organization's goals.
- Assists with the preparation and conducts presentations on role of Division/Unit for the Orientation and Onboarding programme.

Other Responsibilities

- Performs all other duties and functions as may be required from time to time.

5. PERFORMANCE STANDARDS

- Data Protection and privacy legal frameworks, policies, procedures and systems researched, developed and implemented in keeping with established standards and specified timeframes.
- Data Protection/Privacy Governance Frameworks and strategies coordinated in keeping with established standards and specified timeframes.
- Data Protection and privacy advice provided in keeping with established standards and specified timeframes.
- Robust and comprehensive Data Protection controls coordinated in keeping with established standards and specified timeframes.
- Data Protection and privacy training coordinated and provided in keeping with established standards and specified timeframes.
- Reports, Submissions/Notes, technical papers, and publications prepared and issued in keeping with established standards and specified timeframes.
- Stakeholder Relationships and Alliances maintained in keeping with established standards and specified timeframes.
- Technical advice and recommendations provided are sound and supported by qualitative/quantitative data.
- Annual/Quarterly/Monthly performance reports are evidence-based and prepared in accordance with agreed format and submitted on time.
- Individual Work Plan developed in conformity to established standards and within agreed timeframes.
- Confidentiality, integrity and professionalism displayed in the delivery of duties and interaction with staff.

6. AUTHORITY

- Act as primary contact for the organisation, regulators, and public bodies on data protection policies and issues.
- The Data Protection Officer has the authority to investigate and have immediate access to all personal data and data processing operations and to perform his/her duties independently.
- Specifically, the Data Protection Officer must:
 - handle queries or complaints on request by the Judiciary, the controller, other persons, or on his/her initiative.
 - ensure that any other tasks or duties assigned to the Data Protection Officer do not result in a conflict of interest with his/her role as a DPO.

7. INTERNAL AND EXTERNAL CONTACTS (specify purpose of significant contacts)

Internal Contacts

Contact (Title)	Purpose of Communication
Director Court Administration/Chief Executive Officer Director of Court Administration	• Support the CEO and Senior Executives in consultations with the relevant Chief Justice on Data Protection matters, by providing accurate information and interpretation of issues relevant to the delivery of key initiatives and timely responses to sensitive or contentious issues • Collaborate and maintain open relationships to expedite responses and information transfer
Senior Executives/Management	• Provide expert Data Protection advice to influence decisions, support initiatives; • Ensure that executives are fully informed of the organisation's Data Protection initiatives; • Provide expert strategic planning advice to influence decisions, support initiatives.
General Staff	• Develop and maintain effective relationships • Provide expert advice and exchange information

External Contacts

Contact (Title)	Purpose of Communication
Ministry of Justice	• Receive authoritative advice on key policy and legislation initiatives and provides expert operational advice on Data Protection matters;

Contact (Title)	Purpose of Communication
	• Optimize engagement, consultation, negotiation and facilitation of policy and programme alignment, implementation and response; • Collaborate on Data Protection interventions to influence decisions, support initiatives.
Ministries/Departments/Agencies	• Establish effective high-level networks with key stakeholders to enable performance benchmarking, monitor industry trends, maintain currency, and collaborate on common issues to emerging and future issues. • Optimize engagement, consultation, negotiation and facilitation of policy and programme alignment, implementation and response.
Office of the Information Commissioner	• To receive expert Data Protection/Privacy legal/policy/programme development and implementation advice to influence decisions, support initiatives. • To provide a range of reports and other requirements in accordance with the Data Protection Act 2020
Technical Committees	• Foster effective proactive relationships with other stakeholders, in particular community and/or industry groups for whom Data Protection impacts are most critical
Other Stakeholders, example: Professional Bodies, Academia, etc.	• Foster effective proactive relationships with other stakeholders, in particular community and/or industry groups for whom Data Protection impacts are most critical
General Public	• Receive and share information

8. REQUIRED COMPETENCIES

Core

- Excellent interpersonal and team management skills
- Excellent communication skills
- Strong analytical and problem-solving skills
- Strong leadership skills
- Strong customer relations skills

- Excellent planning and organizing skills
- Excellent judgment and decision-making skills
- Ability to influence and motivate others
- Proficiency in the use of relevant computer applications

Technical

- Good knowledge of Data Protection/Privacy legislative arrangements and frameworks.
- Good knowledge of information technology and data management systems.
- Good knowledge and expertise in quantitative and qualitative methodologies, reporting, data quality assessments, data analysis and presentation.
- Good of the development, analysis, revision and implementation of policies, programmes, procedures, guidelines, programmes and legislation.
- Strong ability to synthesize multiple ideas and complex information into a coherent summary, as in reports and briefing notes, and to make cogent recommendations for the modification or creation of legislation, policies and programmes.
- Superior verbal and written communication skills, with the ability to deliver presentations with tact, clarity, enthusiasm and accuracy to widely varied audiences.
- A high level of initiative and self-motivation.
- Demonstrated interpersonal and negotiation skills.
- Aptitude for developing and maintaining collaborative relations with team members both within and outside the Judiciary, and for functioning effectively on inter-ministerial and multi-sectoral committees and working groups.
- Familiarity with procedures, policies and legislation governing the machinery of government.
- Knowledge of the Government processes, including policy development, financial planning, performance management systems and basic theories, principles and methods of analysis.
- Knowledge of computerized systems and software, with an emphasis on the MS Office suite and projects.

9. MINIMUM REQUIRED EDUCATION AND EXPERIENCE

- Bachelor's degree in Data Protection/Privacy, Law, Library & Information Management, Governance, IT Security, Audit or equivalent qualifications.
- At least one Data Protection and/or Privacy certification such as, CIPP, CIPT, ISEB, etc., (preferred).
- Three (3) years' experience in compliance, audit and/or risk management, or equivalent experience.

10. SPECIAL CONDITIONS ASSOCIATED WITH THE JOB

- Work will be conducted in an office outfitted with standard office equipment and specialized software. The environment is fast paced with on-going interactions with critical stakeholders and meeting tight deadlines which will result in high degrees of pressure, on occasions. May be required to travel locally and overseas to attend conferences, seminars and meetings.